



(11) **EP 2 289 239 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
19.03.2014 Bulletin 2014/12

(51) Int Cl.:
H04N 7/16 (2011.01)

(21) Application number: **09749818.2**

(86) International application number:
PCT/EP2009/056041

(22) Date of filing: **19.05.2009**

(87) International publication number:
WO 2009/141328 (26.11.2009 Gazette 2009/48)

(54) **METHOD FOR THE ALLOCATION AND MANAGEMENT OF SUBSCRIPTIONS FOR THE RECEPTION OF BROADCAST PRODUCTS**

VERFAHREN FÜR DIE ZUWEISUNG UND VERWALTUNG VON ABONNEMENTS FÜR DEN EMPFANG VON RUNDfunkPRODUKTEN

PROCÉDÉ D'ATTRIBUTION ET DE GESTION D'ABONNEMENTS POUR LA RÉCEPTION DE PRODUITS RADIODIFFUSÉS

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL
PT RO SE SI SK TR**

(30) Priority: **21.05.2008 EP 08156700**
27.05.2008 US 56314 P

(43) Date of publication of application:
02.03.2011 Bulletin 2011/09

(73) Proprietor: **Nagravision S.A.**
1033 Cheseaux-sur-Lausanne (CH)

(72) Inventor: **MOREILLON, Guy**
CH-1042 Bioley-Orjulaz (CH)

(74) Representative: **Wenger, Joel-Théophile**
Leman Consulting S.A.
Chemin de Précossy 31
1260 Nyon (CH)

(56) References cited:
EP-A- 1 109 405 EP-A- 1 411 727
EP-A- 1 638 331 EP-A- 1 662 789
EP-A- 1 775 950 EP-A- 1 853 000
WO-A-02/062054 FR-A- 2 894 745
US-A1- 2004 052 377 US-A1- 2004 240 394
US-B1- 6 466 671

EP 2 289 239 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

Introduction

[0001] This invention concerns the management of a set of subscribers to broadcast services subject to conditional access.

Prior art

[0002] Visual or audio services are transmitted in the form of a data flow to receivers, such as home receivers (set-top-box) or mobile receivers. By way of example a data flow could be a stock-exchange data service, a weather forecast, general-purpose television, a sports event broadcast and so on. These contents can be broadcast on user units such as a Pay-TV decoder, a computer or even a mobile phone, a "palm-top", a PDA, a radio, a television, a multimedia terminal.

[0003] The digital data flow is encrypted in order to be able to restrict the use and define the conditions for such use. This encryption is accomplished thanks to control words which are changed at regular interval (between 5 and 30 seconds) in order to dissuade any attack aimed at discovering such control words.

[0004] In order to allow the user unit to decipher the data flow encrypted by a control word, the latter is sent independently of the data flow in a control message (ECM) encrypted by a key used in the system allowing for the transmission between the management centre (CAS) and the security module of the user unit. Indeed, the security operations are carried out in a security module (SC) which is a tamper-proof device. This module processes the messages related to the rights of the receiver.

[0005] At the time of the decryption of the control message (ECM), the right of access to the considered data flow is verified in the security module (SC). The control word is returned in clear to the user unit only when the verification is positive.

[0006] As is well known to a person skilled in the art, the security module can essentially be realized according to any of four distinct forms. One such form is a micro-processor card, a smart card, or more generally an electronic module (having a form of key, or a badge etc). Such a module is connectable and generally removable from the decoder. The form with electric contact is the most used, but the version without contact for instance of type ISO 14443 is also used. It can also take the form of an SD card, microSD, MMC, Memory stick or any other form of memory card.

[0007] In a second known form, the security module is integrated in an electronic circuit package, mounted generally in a permanent and non-removable way in the decoder box. An alternative is made of a circuit package mounted on a connector such as a SIM module connector.

[0008] In a third form, the security module is integrated in an integrated circuit package having also another func-

tion, for instance in the decoder's descrambling module or the decoder's microprocessor.

[0009] In a fourth embodiment, the security module is not physically realized, but its function is implemented in the form of software. Given that in the four cases, although the security level differs, the function is identical, we can refer to security module whatever way its function is realized or the form that this module takes.

[0010] The reception rights are generally managed by authorization messages (EMM) which are loaded into the security module (SC). Other possibilities are also possible such as sending decryption keys.

[0011] It is well known that such security modules include a unique identification number UA0 loaded into the memory during an initialization phase. At the time of the subscription to a television service, the security module (SC) receives a subscriber identification number UA1 which will be used later in a group addressing method.

[0012] According to an example in which the size of the group of subscribers is 512, the 9 lower bits of the subscriber identification number UA1 will be ignored and the receiver will filter the address of UA1 based on the bits of higher significance than that of the 9th bit.

[0013] It is the subscriber identification number UA1 which will serve to address the security module in a group basis, the unique number UA0 taking part if individual addressing is necessary. This is the case at the time of a subscription modification, for instance the recording in the security module of a subscription right for a new product.

[0014] Thus, the receiver will configure its message filter in order to pass the messages containing in the header the unique identification number UA0 or the subscriber identification number UA1. These numbers are transmitted by the security module to the receiver in order to initialize its filter.

[0015] The subscription management is managed according to the principle of rights renewal i.e. that rights are linked with an expiry date after which the security module refuses to consider his rights as valid. In order for the subscriber to be able to continue to take advantage of his subscription without interruption it is thus necessary to transmit a rights renewal message (in so far as the subscriber has the right to receive it) postponing the expiry date till later.

[0016] In practice, the duration of a renewal is typically 1 month, which means that all the receivers must receive a renewal message within a month. Since we are in a broadcast environment, the management centre does not know when the receivers are switched on and this is the reason why the messages are repeated many times.

[0017] To reduce the number of message to be sent, it has been proposed to use group addressing rather than individual addressing. Take the example of a provider proposing 5 products for subscription. It will then be necessary to send 5 rights renewal messages per group, each message comprising the renewal conditions for a product. Since not all the group members will have sub-

scribed to the product related to this message, a group message thus comprises a field of type bitmap with one bit dedicated to each member of the groups. If a group contains 256 members, the bitmap field will contain 256 bits, each bit being attributed to a specific security module.

[0018] The security module, at the time of reception of the group message, will first verify if its own bit is at 1 to know if the renewal command is intended for it. If the bit is at 0, it will ignore the renewal control, or even clear the subscription right considered by this message.

[0019] It is apparent that such a message is encrypted and that only the security modules have access to the key to decrypt it. Moreover, the message contains authentication data ensuring that only the designated authority can generate such message. This is done thanks to asymmetrical key cryptography.

[0020] One of the problems encountered is of course the large number of renewal messages to be sent and therefore the use of available bandwidth, the latter being best used for audiovisual services. In our example with 5 products, each subscriber having subscribed to one product, the bitmap will be on average filled to 20% with 1's and to 80% with 0's, given that the products are uniformly distributed among the subscribers. This is the ideal situation and is rather unlikely. The bitmap will in fact have a unpredictable structure, some groups having a large number of participants having subscribed for a specific product and other groups having a small number of participants having subscribed to this same product. This entropy makes the compression of the bitmap very difficult.

[0021] One can imagine the necessary bandwidth when more than 2 million subscribers should be managed. An approach therefore consists in increasing the size of the groups (1024 or more) to reduce the number of messages but it will then be necessary to increase the size of the messages to be able to contain a bitmap of 1024 or even more, thus having the effect of increasing the bandwidth used by these messages and reducing the gain achieved by the group messaging technique. It can be seen that the increase of the group size can only be a partial solution.

[0022] Another problem which has been observed is the volatility rate of the client-base which subscribe and then unsubscribe some months later. The subscription number initially allocated to such a subscriber can no longer be used. Indeed, the rights are still present in the first receiver (or security module) at the moment of the end of the subscription. To bypass the access control system, the owner needs simply to interrupt the reception of the messages containing a zero in the bitmap signalling an erase command. If this subscription number is furthermore reallocated to a second receiver some months later, the first receiver needs simply to be switched on in order for the renewal messages to be received and for the rights to be unjustly updated, allowing for the undue reception of audiovisual services.

[0023] To avoid this, the number allocated to a subscriber is no longer used after its expiry. The arrival of new subscribers leads to the creation of new groups while older groups shrink and contain only a few subscribers for which it is nevertheless necessary to send a group message.

[0024] The document US 6,466,671 is an illustration of the method leading to the huge number of renewal messages.

[0025] This document describes a distribution system for broadcast contents. The receiver comprises a security module having a subscriber identification number UA. The subscriber management system is in charge of sending to each receiver the rights or keys allowing to access the content for which this receiver is authorized. At the initialization, a receiver, more particularly its security module, is identified by its unique identifier. Three types of messages are disclosed, individual messages, group messages or all audience messages. The group message comprises a bitmap to address each member of this group. A group subscription bitmap is set up according to the contents of the subscriber database. The individual bits in the bitmap are set to 1 or zero according to whether or not the particular subscriber is to have his rights renewed. The Message Generator sets an obsolescence date to indicate to the smartcard the date beyond which the particular subscription EMM is not valid. The security module is arranged to compare this date with the current date which is contained in received ECMs and to prevent decryption if the current date is later than the obsolescence date.

Brief description of the invention

[0026] The aim of the present invention is to propose a method to reduce the bandwidth necessary for the renewal of subscriptions to the reception of broadcast services.

[0027] This aim is achieved by a method for the allocation and management of subscriptions to a plurality of products for at least one receiver comprising a security module, this module comprising a unique identification address UA0, this method being carried out by a management centre and comprising the following steps:

- defining a plurality of sets of subscriber identification numbers AB, each set being associated with a product,
- splitting a set of subscriber identification numbers into groups of subscribers,
- searching for an available subscriber identification number AB_k related to the desired product at the time of the initialization of a new subscriber,
- determining if this available number has already been previously allocated,

- if so, determining if an inhibit duration has elapsed between the end of the previous subscription and the start of the new subscription, if not, searching for a new number,
- sending an initialisation message to the new subscriber addressed according to his unique identification address UA0 and containing the subscriber identification number ABk of his product as well as the right to said product,
- preparing a group rights renewal message for the product to the group containing the subscriber identification number ABk, this message comprising the group header containing this subscriber ABk and a bitmap allowing to individually address each of the group members,
- compressing the bitmap and adding the compressed bitmap to the message,
- sending the renewal message.

[0028] By product, we mean a subscription to a television channel, a plurality of channels or a television event series (e.g. football season, serials, episodes).

[0029] Thus the management centre does not manage a range of subscriber numbers common to all products but a specific range per product. Consequently, the groups constituting subscribers of a product will, in principle, be full. Advantageously, group messages will affect a large majority of members of a group. Another advantage is that the bitmap will be compressible since it is formed, for the most part, by active bits (bits set to one).

[0030] The reasons leading to a group not being full are the following:

- creation of a new group at the time of the arrival of new clients
- cancellation by a member of the group, this number still being within the inhibit duration.

Brief description of the drawings

[0031] The invention will be better understood thanks to the following detailed description and with reference to the attached drawings which are given as a non-limiting example, namely:

- Figure 1 shows the case of a renewal before the expiry date,
- figure 2 shows the case of a renewal after the expiry date,
- figure 3 shows the case of a renewal message arriving after the inhibit date.

Detailed description

[0032] The invention is divided into two parts cooperating together.

5 **[0033]** The first part of the invention is carried out in the management centre and is based on the method for the allocation of a subscriber number at the time of the conclusion of a contract. This method is also carried out at the modification of a product for a subscriber or the conclusion of a subsequent subscription.

10 **[0034]** At the time of the initial definition of the range numbers by product, a range is divided into groups (for example 2048 members) each number is indexed in a database with management data. One of these data concerns the above mentioned inhibit predetermined duration.

15 **[0035]** This duration is used by the security module, member of a group, according to the following method:

- 20 - receiving at least one group rights renewal message for at least one product by the security module, said security module being a member of said group, this message containing an expiry date for the rights to said product and a current date,
- 25 - verifying that the group rights renewal message authorizes the renewal of the rights for said security module,
- 30 - verifying that the current date is before an inhibit date, if so:
- replacing the expiry date of said rights with the received expiry date,
- 35 - generating a new inhibit date by adding an inhibit duration to the current inhibit date, in such a way that the new inhibit date is after the new expiry date.

40 **[0036]** This module comprises a unique address UA0 and at least a subscriber address ABx which is allocated when someone takes out a subscription for the product X. The module will therefore receive as many subscriber addresses as the subscriber subscribes to products.

45 **[0037]** It is this addressing method which will be used to send personalized messages (single message addressed to UA0) or group messages (shared messages addressed to ABn). A group message includes in its header a product identifier which is compared, by the receiver, with the identification of products to which the subscriber of this security module has subscribed. The subscriber's security module will also be a member of this group for that product in order to receive this kind of message. Since this message is addressed to a group (usually of 256, 512, 1024 or even 2048 participants), this message also includes data pertaining to each security module which has the form of a bitmap. 512 bits are placed in the message (for the example to 512 par-

ticipants) and each security module knows which of the bits is the one that concerns it. The message contains the starting address of the bitmap and the 512 bits of the bitmap allow to address specifically the 512 participants following the starting address. Thus the command contained in the message is addressed to a subset (or all) of the group designated by the bitmap. According to this, in case that a right should be renewed, one put the bit in the bitmap is set to 1 for all the members of the group for which the renewal is authorized and to zero for the others.

[0038] At the time of the reception of a renewal message, once the message for its group received, the security module will verify in the bitmap if the command in the message is addressed to it. Once this verification is made, the inhibit date is verified in order to determine if this command is still valid for the security module.

[0039] It is to be noted that the renewal message includes a current date which will be used for comparisons.

Figure 1 shows the case where the current date of the message falls before the end of the expiry date RDate for the right. The current date of the renewal message being before the expiry date, the right is prolonged as well as the inhibit date EDate as illustrated on the second line. The authorization period of the service (or product) related to this right is illustrated in grey indicating that no interruption has taken place.

Figure 2 shows the case where the current date of the renewal message falls after the expiry date RDate but before the inhibit date EDate. It can be seen on the grey part that from the first expiry date till the arrival of the renewal message MSG, the authorization to the service is interrupted. Once the message is processed, the authorization is enabled till the new expiry date RDate.

[0040] In Figure 3 we see the case where the current date of the renewal message is situated after the inhibit date EDate. In this case the renewal is ignored and the last expiry date defines the end of the authorization to the service.

[0041] According to an embodiment, a renewal message in which the bit related to this security module of the bitmap is set to zero causing the update of the expiry date RDate to the current date of the message and this causes the ending of the authorization related to the right. Indeed, the subsequent control messages, containing the control words and the description of the rights necessary for releasing this control word will comprise a date which will be after the expiry date RDate.

[0042] According to an embodiment, the security module includes a single date which is the expiry date RDate. Moreover, it includes an inhibit duration defined in day (s) or month(s) for instance which allows the security module to calculate the inhibit date when a renewal message is received. The inhibit date is thus calculated as the sum of the expiry date RDate and the inhibit duration.

[0043] It is thus not necessary to update two dates during a renewal operation. The inhibit duration can be defined at the time of the initialization of the security module, for instance with the initial loading of the rights.

[0044] According to another embodiment of the invention, the update of a new inhibit date by adding a predefined duration to the current inhibit date is done at the management centre and the new inhibit date is contained in the renewal message. The new inhibit date is extracted for the message and stored in the security module.

[0045] Thanks to the method described above working in a security module, it is now possible to reuse an identification number of a given subscriber. Take the example of a subscriber terminating his subscription the on the 30th of June. The expiry date RDate is thus fixed at 30th June by the renewal of the previous date, for instance the 30th of May. The group messages destined for the group to which the security module belongs, sent during the month of June, will contain a zero in the bit of the bitmap relating to this security module. No renewal will then be carried out during the month of June. The inhibit date is it fixed at the 30th of July with a difference of one month relative to the expiry date (1 month = inhibit duration).

[0046] The management system can thus attribute the subscriber identification number ABk to another subscriber, knowing that after the 30th of July, even if a renewal message were to be accepted by this security module (bitmap to 1), the renewal will not be carried out.

[0047] Thus, thanks to this mechanism, the members of the group are by and large active subscribers, the unique condition being to reserve the identification number of a subscriber having terminated his subscription during the time that the inhibit date is past. At the time of the allocation of a new subscriber identification number related to a given product, preference will be given to a group not having reached the threshold, allows for the efficient compression of the bitmap.

[0048] In order for the bitmap to be efficiently compressed, it should be homogeneous. Thus large numbers of consecutive 0's in the bitmap contribute to the homogeneity. In the same way, a group which is linearly filled, each subscriber following the previous one (as far as the subscriber identification number is concerned), allows for an optimal compression since a consecutive part of the bitmap is filled with 1's and the other part is filled with 0's (00000000...0000011111...1111111)

[0049] Thereby the bitmap of this group can be efficiently compressed onto a few bytes in spite of the large size of the group, more than 2048 bits (more than 256 bytes).

Claims

1. Method for the allocation and management of subscriptions to Pay-TV offer for at least one receiver comprising a security module, this module compris-

ing a unique identification address (UA0), this method being carried out by a management centre and comprising the following steps:

- splitting the Pay-TV offer into a plurality of products, each product being associated with a unique subscription, 5
- defining a set of subscriber identification numbers (AB), each set being associated with one product, 10
- splitting a set of subscriber identification numbers into groups of subscribers,
- searching for an available subscriber identification number AB_k related to the desired product at the time of the initialization of a new subscription, 15
- determining if this available number has already been previously allocated,
- if so, determining if an inhibit duration has elapsed between the end of the previous subscription and the start of the new subscription, if not, searching for a new number, 20
- sending an initialization message to the new subscriber addressed according to his unique identification address (UA0) and containing the subscriber identification number (AB_k) of his product as well as the subscription right to said product, 25
- preparing a group rights renewal message for the product for the group containing the subscriber identification number AB_k, this message comprising the group header containing this subscriber AB_k and a bitmap allowing to individually address each member of the group, **this message comprising an expiry date for the rights to said product and a current date**, 30
- compressing the bitmap and adding the compressed bitmap to the message,
- sending the group renewal message,
- receiving the group rights renewal message for at least one product by the security module, said security module being a member of said group, 40
- verifying that the group rights renewal message authorizes the renewal of the rights for said security module **by checking the corresponding bit of the bitmap, if so:** 45
- verifying that the current date is before an inhibit date, if so: 50
- replacing the expiry date of said rights with the received expiry date, **and**
- generating a new inhibit date by adding **the** inhibit duration to the current inhibit date, in such a way that the new inhibit date is after the new expiry date. 55

2. Method for the allocation and management of sub-

scriptions according to claim 1, **characterized in that** the generation of the new inhibit date includes the following steps:

- calculating at the management centre of a new inhibit date by adding a predetermined duration to the current inhibit date,
- inserting the new inhibit date in the renewal message,
- extraction, by the security module, of the new inhibit date from the renewal message and updating the expiry date in the security module..

3. Method for the allocation and management of subscriptions according to claim 1, **characterized in that** the updating of the new inhibit date includes the following steps:

- determining an inhibit duration by the management centre and inserting said inhibit duration in the rights initialization message,
- extracting the inhibit duration of the initialization message by the security module and storage of same,
- at the time of the updating of the expiry date, calculating the new inhibit date by summing the new expiry date and the inhibit duration,
- storing the new inhibit date in the security module.

Patentansprüche

1. Verfahren zur Zuteilung und Verwaltung von Abonnements auf ein Pay-TV-Angebot für mindestens einen Empfänger mit einem Sicherheitsmodul, wobei dieses Modul eine eindeutige Identifizierungsadresse UA0 umfasst, und wobei dieses Verfahren von einem Verwaltungszentrum mit den folgenden Phasen durchgeführt wird:

- Unterteilung des Pay-TV-Angebots in eine Vielzahl von Produkten, wobei jedes Produkt mit einem Abonnementprodukt verbunden ist,
- Definierung eines Satzes von Abonnenten-Identifizierungszahlen (AB), wobei jeder Satz mit einem Produkt verbunden ist,
- Unterteilung eines Satzes von Abonnenten-Identifizierungszahlen in Gruppen von Abonnenten,
- Suche nach einer verfügbaren Abonnentenidentifizierungs-Zahl AB_k bezogen auf das gewünschte Produkt zum Zeitpunkt der Initialisierung eines neuen Abonnenten,
- Ermittlung, ob diese verfügbare Zahl schon vorher zugewiesen wurde,
- wenn ja, Ermittlung, ob eine Verhinderungsdauer zwischen dem Ende des vorherigen

Abonnements und dem Beginn des neuen Abonnements verstrichen ist, wenn nicht, Suche nach einer neuen Zahl,

- Sendung einer Initialisierungsnachricht an den neuen Abonnent, die mit seiner eindeutigen Identifizierungsadresse UA0 adressiert ist und die Abonnentenidentifizierungs-Zahl ABk seines Produkt sowie das Recht auf das Produkt enthält,

- Vorbereitung einer Nachricht über die Erneuerung der Gruppenberechtigungen für das Produkt für die Gruppe, die die Abonnentenidentifizierungs-Zahl ABk enthält, wobei diese Nachricht die Gruppenüberschrift umfasst, die diesen Abonnenten ABk enthält, sowie eine Bitmap, die es gestattet, jedes Mitglied der Gruppe einzeln anzusprechen, wobei diese Nachricht ein Ablaufdatum für die Rechte auf besagtes Produkt sowie das laufende Datum umfasst,

- Komprimieren der Bitmap und Hinzufügen der komprimierten Bitmap zu der Nachricht,

- Senden der Gruppen-Erneuerungsnachricht, - Empfang mindestens einer Nachricht über die Erneuerung der Gruppenberechtigungen für mindestens ein Produkt durch das Sicherheitsmodul, wobei das Sicherheitsmodul ein Mitglied der Gruppe ist,

- Prüfung, ob die Nachricht über die Erneuerung der Gruppenberechtigungen zur Erneuerung der Berechtigungen für besagtes Sicherheitsmodul ermächtigt, mittels Prüfung des entsprechenden Bits der Bitmap,

- Prüfung, ob das aktuelle Datum vor einem Verhinderungsdatum liegt; wenn ja:

- Ersetzung des Ablaufdatums der Berechtigungen durch das empfangene Ablaufdatum,

- Erzeugung eines neuen Verhinderungsdatums durch Hinzufügen einer Verhinderungsdauer zu dem derzeitigen Verhinderungsdatum, so dass das neue Verhinderungsdatum nach dem neuen Ablaufdatum liegt.

2. Verfahren zur Zuteilung und Verwaltung von Abonnements gemäß Anspruch 1, **gekennzeichnet dadurch, dass** die Erzeugung des neuen Verhinderungsdatums die folgenden Phasen umfasst:

- im Verwaltungszentrum Berechnung eines neuen Verhinderungsdatums durch Hinzufügen einer vorherbestimmten Dauer zu dem derzeitigen Verhinderungsdatum,

- Einfügung des neuen Verhinderungsdatums in die Erneuerungsnachricht,

- Extraktion, durch das Sicherheitsmodul, des neuen Verhinderungsdatums aus der Erneuerungsnachricht und Aktualisierung des Ablaufdatums im Sicherheitsmodul.

3. Verfahren zur Zuteilung und Verwaltung von Abonnements gemäß Anspruch 1, **gekennzeichnet dadurch, dass** die Aktualisierung des neuen Verhinderungsdatums die folgenden Phasen umfasst:

- Ermittlung einer Verhinderungsdauer durch das Verwaltungszentrum und Einfügung besagter Verhinderungsdauer in die Nachricht über die Initialisierung der Rechte,

- Extrahieren der Verhinderungsdauer aus der Initialisierungsnachricht durch das Sicherheitsmodul und Lagerung derselben,

- bei der Aktualisierung des Ablaufdatums Berechnung des neuen Verhinderungsdatums, indem man das neue Ablaufdatum und die Verhinderungsdauer zusammenzählt,

- Speichern des neuen Verhinderungsdatums im Sicherheitsmodul.

Revendications

1. Méthode d'allocation et de gestion d'abonnements à une offre de télévision à péage pour au moins un récepteur comprenant un module de sécurité, ce module comprenant une adresse d'identification unique (UAO), cette méthode étant mise en oeuvre par un centre de gestion et comprenant les étapes suivantes :

- séparation de l'offre de télévision à péage en une pluralité de produits, chaque produit étant associé à un abonnement unique,

- définition d'un ensemble de numéros d'identification d'abonnés (AB), chaque ensemble étant associé à un produit,

- séparation d'un ensemble de numéros d'identification d'abonnés en groupes d'abonnés,

- recherche d'un numéro d'identification d'abonné disponible ABk relatif au produit désiré au moment de l'initialisation d'un nouvel abonnement,

- détermination si ce numéro disponible a déjà été attribué précédemment,

- dans l'affirmative, déterminer si une durée de blocage s'est écoulée entre la fin de l'abonnement précédent et le début du nouvel abonnement, dans la négative, rechercher un nouveau numéro,

- envoi d'un message d'initialisation au nouvel abonné adressé selon son adresse d'identification unique (UAO) et contenant le numéro d'identification d'abonné (ABk) de son produit en plus du droit pour ce produit,

- préparation d'un message de groupe de renouvellement de droits pour le produit destiné au groupe contenant le numéro d'identification d'abonné ABk, ce message comprenant le pré-

fix du groupe contenant cet abonné ABk et un bitmap permettant d'adresser individuellement chaque participant du groupe, ce message comprenant une date d'expiration des droits pour ce produit, ainsi qu'une date courante, 5

- compression du bitmap et adjonction du bitmap compressé au message,
- envoi du message de groupe de renouvellement,
- réception par le module de sécurité, du message de groupe de renouvellement de droit pour au moins un produit, ce module de sécurité étant membre dudit groupe, 10
- vérification que le message de groupe de renouvellement des droits autorise le renouvellement des droits pour ledit module de sécurité en vérifiant le bit correspondant du bitmap, et dans l'affirmative : 15

○ vérification que la date courante est antérieure à une date de blocage, dans l'affirmative: 20

■ remplacement de la date d'expiration desdits droits par la date d'expiration reçue, et 25

■ génération d'une nouvelle date de blocage par addition de la durée d'inhibition à la date de blocage courante, de sorte que la nouvelle date de blocage soit postérieure à la nouvelle date d'expiration. 30

2. Méthode d'allocation et de gestion d'abonnements selon la revendication 1, **caractérisée en ce que** la génération de la nouvelle date de blocage comprend les étapes suivantes : 35

- calcul au centre de gestion d'une nouvelle date de blocage par addition d'une durée prédéterminée à la date de blocage courante, 40
- insertion de la nouvelle date de blocage dans le message de renouvellement,
- extraction de la nouvelle date de blocage par le module de sécurité à partir du message de renouvellement et mise à jour de la date d'expiration dans le module de sécurité. 45

3. Méthode d'allocation et de gestion d'abonnements selon la revendication 1, **caractérisée en ce que** la mise à jour de la nouvelle date de blocage comprend les étapes suivantes : 50

- détermination d'une durée de blocage par le centre de gestion et insertion de ladite durée de blocage dans le message d'initialisation des droits, 55
- extraction de la durée de blocage du message

d'initialisation par le module de sécurité et stockage de cette durée de blocage,

- lors de la mise à jour de la date d'expiration, calcul de la nouvelle date de blocage par addition de la nouvelle date d'expiration et la durée de blocage,
- stockage de la nouvelle date de blocage dans le module de sécurité.

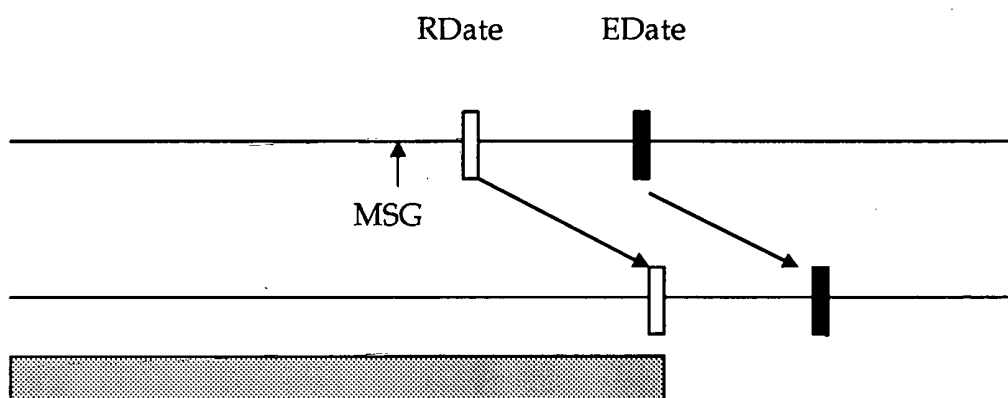


Fig. 1

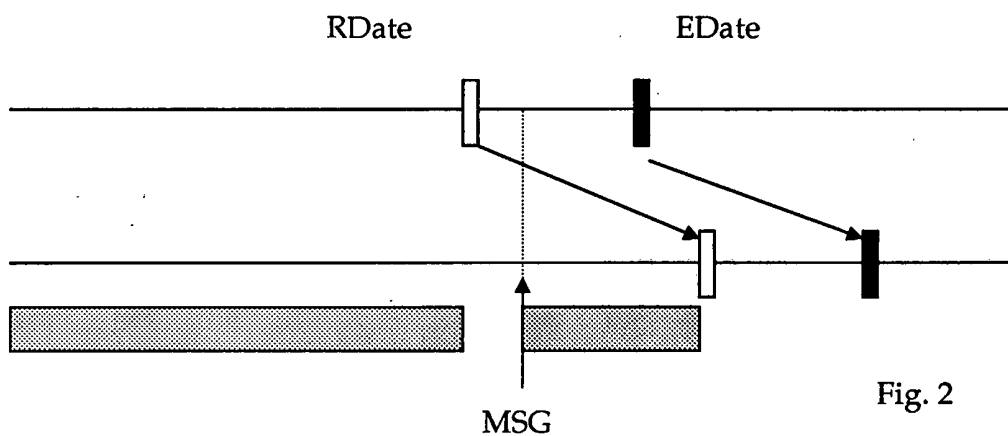


Fig. 2

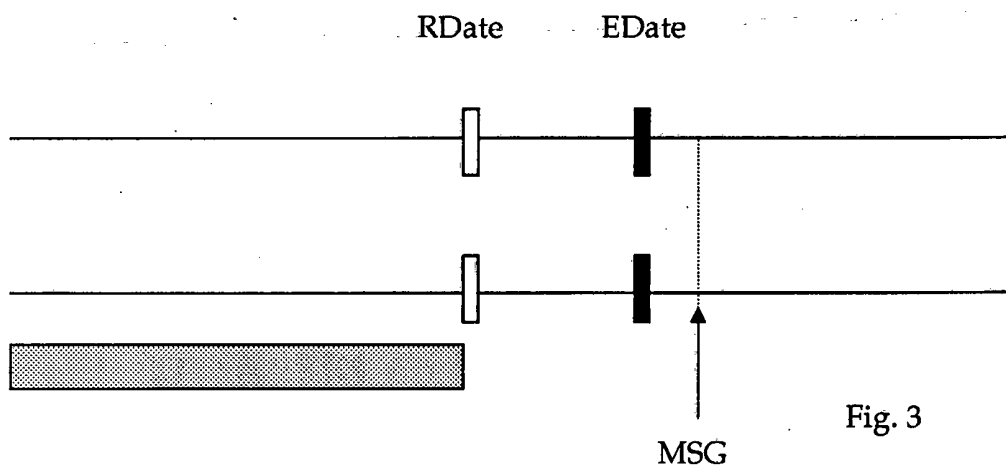


Fig. 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6466671 B [0024]